SYSTEMS AND METHODS FOR RESERVING CRYPTOGRAPHIC KEY MATERIAL

GOVERNMENT CONTRACT

[0001] The U.S. Government has a paid-up license in this invention and the right in limited circumstances to require the patent owner to license others on reasonable terms as provided for by the terms of Contract No. F30602-01-C-0170, awarded by the Defense Advanced Research Projects Agency (DARPA).

TECHNICAL FIELD

[0002] The invention relates generally to the field of cryptographic systems, and more particularly to systems and methods for reserving a rate at which secret bits are provided for one or more applications that consume the secret bits.

BACKGROUND OF THE INVENION

[0003] Advantage distillation is a well-known approach to a cryptographic key agreement protocol. An example of a system that exploits advantage distillation is a quantum cryptographic system, although other exemplary systems, such as those based on receiving random or pseudo-random sequences of 0s and 1s from satellite or terrestrial transmissions, including radio frequency (RF) transmissions, have also been proposed.

[0004] A system that exploits advantage distillation may include a source of bits (S) and two legitimate receivers (A, B). If an eavesdropper (E) does not have perfect reception of the random bits (S), then A and B can agree on random numbers derived

from the S bits in such a way that E essentially has no knowledge of the random numbers, even if E has a much better receiver than A or B.

[0005] In order to perform advantage distillation, A and B communicate via a public communications channel regarding the bits they received well. The well-received bits are used to create a shorter random number. The greater the ratio of the original length of the random sequence to this shorter random number, the greater the assurance that E will have little or no knowledge of the shorter random number.

[0006] Such a system may use a flow of secret bits that may be used as cryptographic key material to which the system adds and consumes over time. Such systems provide the key material on a first-come, first-served basis. It would be advantageous for a process that requires a flow of secret bits to be able to reserve a particular rate of secret bits in order to guarantee the availability of the secret bits to the process when needed. Current systems that exploit advantage distillation do not provide such a feature.

SUMMARY OF THE INVENTION

[0007] Systems and methods are provided for reserving a rate at which secret bits are provided for applications that consume the secret bits. Such applications may include cryptographic applications, such as those that are based on advantage distillation (for example, an application that employs quantum cryptography). Typically, such applications may include a secret bits producing application for producing the secret bits and may include an application, such as a client application, that consumes the secret bits produced by the secret bits producing application.

[0008] In a first aspect of the invention, a method is provided for reserving a rate at which cryptographic material is provided. A first reservation request for reserving a first rate is sent from a first secret bits consuming application to a secret bits producing application. The secret bits producing application determines whether the reservation request can be satisfied. When the secret bits producing application determines that the reservation request can be satisfied, the first rate is reserved for the first secret bits consuming application.

[0009] In a second aspect of the invention, a system is provided. The system includes a secret bits consuming application and a secret bits producing application. The secret bits producing application is configured to receive a request from the secret bits consuming application for a reservation of a rate of secret bits to be produced by the secret bits producing application. The secret bits producing application is further configured to determine whether the reservation can be satisfied and to send a notification to the secret bits consuming application when the reservation request can be satisfied.

[0010] In a third aspect of the invention, a machine-readable medium having instructions recorded thereon is provided. When the instructions are read and executed by at least one processor, the at least one processor performs servicing a reservation request for reserving a rate at which secret bits are provided for a secret bits consuming application, determining whether the reservation request can be successfully serviced, and reserving the rate for the bits consuming application when the reservation request can be successfully serviced.

[0011] In a fourth aspect of the invention, a system is provided. The system includes means for producing secret bits for use in a cryptographic system and means for using the secret bits to cryptographically protect traffic to be sent through a network. The means for producing the secret bits includes means for receiving a reservation request from the means for using the secret bits and means for reserving the bit rate at which the secret bits are provided and notifying the means for using of a successful reservation.

[0011] In a fifth aspect of the invention, a method of reserving a rate of providing cryptographic key material is provided. A desired consumption rate of cryptographic key material is specified at a first network device. The desired consumption rate of cryptographic material is reserved.

[0012] In a sixth aspect of the invention, a method of reserving a rate of providing secret bits from a secret bits producer based on advantage distillation is provided. A first process specifies a desired rate. A secret bit producer based on advantage distillation reserves the desired rate.

[0013] In a seventh aspect of the invention, a method of reserving a rate of generated cryptographic key material from an advantage-distillation based secret bits producer is provided. The advantage-distillation based secret bits producer generates cryptographic key material. A request from a secure communication process for a reservation of the cryptographic key material at a first rate is received. The secure communication process is notified of a successful reservation when an available generated rate of cryptographic key material is greater than or equal to a specified minimum acceptable rate.

[0014] In an eighth aspect of the invention, a method of reserving a rate of providing secret key material for protecting communications is provided. A client process specifies

a minimum desired consumption rate of secret key material and a priority. A secret key material producing process determines whether the minimum desired consumption rate of secret key material is available to the client process. When the minimum desired consumption rate of secret key material is not available to the client process, the minimum desired consumption rate of secret key material is made available by canceling at least one previously made reservation of a consumption rate of the secret key material. Each of the at least one previously made reservation has a lower priority than the priority specified by the client process. At least the minimum desired consumption rate of the secret key material is reserved for the client process.

BRIEF DESCRIPTION OF THE DRAWINGS

[0015] The accompanying drawings, which are incorporated in and constitute a part of this specification, illustrate an embodiment of the invention and, together with the description, explain the invention. In the drawings,

[0011] Fig. 1 illustrates an exemplary network consistent with principles of the invention;

[0012] Fig. 2 is a functional block diagram of an exemplary QKD endpoint that may be included in the exemplary network of Fig. 1;

[0013] Fig. 3 is a functional block diagram that illustrates an exemplary configuration of the quantum cryptographic transceiver of Fig. 2 consistent with the principles of the invention,

[0014] Fig. 4 illustrates an exemplary functional block diagram of the QKD endpoint of Fig. 2;

[0015] Fig. 5 is a high-level system diagram of an implementation consistent wit the principles of the invention;

[0016] Fig. 6 illustrates an exemplary format of a reservation table that may be used in implementations consistent with the principles of the invention;

[0017] Fig. 7 illustrates an exemplary REQUEST message that may be used in implementations consistent with the principles of the invention;

[0018] Fig. 8 illustrates an exemplary REPLY message that may be used in implementations consistent with the principles of the invention;

[0019] Fig. 9 illustrates an exemplary DONE message that may be used in implementations consistent with the principles of the invention;

[0020] Fig. 10 is a flowchart of an exemplary process for estimating a production rate and an available rate that may be used in implementations consistent with the principles of the invention;

[0021] Figs. 11, 12A and 12B are flowcharts of an exemplary process for processing a REQUEST message in implementations consistent with the principles of the invention; and

[0022] Fig. 13 is a flowchart of an exemplary process for processing a DONE message in implementations consistent with the principles of the invention.

DETAILED DESCRIPTION

[0023] The following detailed description of the invention refers to the accompanying drawings. The same reference numbers in different drawings may identify the same or

similar elements. The following detailed description does not limit the invention. Instead, the scope of the invention is defined by the appended claims and equivalents.

Exemplary Network

[0024] Fig. 1 illustrates an exemplary network 100 in which systems and methods consistent with principles of the invention may be implemented. Network 100 may include QKD (Quantum Cryptographic Key Distribution) endpoints 105a and 105b connected via a network 110 and an optical link/network 115. QKD endpoints 105a and 105b may each include a host or a server (e.g., a Virtual Private Network (VPN) gateway). QKD endpoints 105a and 105b may further connect to local area networks (LANs) 120 or 125. LANs 120 and 125 may further connect hosts 130a– 130c and 135a –135c, respectively.

[0025] Network 110 can include one or more networks of any type, including a Public Land Mobile Network (PLMN), Public Switched Telephone Network (PSTN), LAN, metropolitan area network (MAN), wide area network (WAN), Internet, or Intranet, a VPN, an ATM network, a network employing MultiProtocol Label Switching (MPLS), an Ethernet network, and a Synchronous Optical Network (SONET). Network 110 may also include a dedicated fiber link or a dedicated freespace optical or radio link. The one or more PLMNs may further include packet-switched sub-networks, such as, for example, General Packet Radio Service (GPRS), Cellular Digital Packet Data (CDPD), and Mobile IP sub-networks.

[0026] Optical link/network 115 may include a link that carries light throughout the electromagnetic spectrum, including light in the human visible spectrum and light beyond the human-visible spectrum, such as, for example, infrared or ultraviolet light. The link

may include, for example, a conventional optical fiber. Alternatively, the link may include a free-space optical path, such as, for example, a path through the atmosphere or outer space, or even through water or other transparent media. As another alternative, the link may include a hollow optical fiber that may be lined with photonic band-gap material.

[0027] QKD endpoints 105 may distribute cryptographic key symbols via optical link/network 115. Subsequent to quantum key distribution via optical link/network 115, QKD endpoint 105a and QKD endpoint 105b may cryptographically protect traffic using the distributed key(s) and transmit the traffic via network 110. Though only two QKD endpoints 105 are shown, multiple QKD endpoints 105 (i.e., more than two) may be present in network 100.

[0028] It will be appreciated that the number of components illustrated in Fig. 1 are provided for explanatory purposes only. A typical network may include more or fewer components than are illustrated in Fig. 1.

Exemplary QKD Endpoint

[0030] Fig. 2 illustrates exemplary components of a QKD endpoint 105 consistent with the present invention. QKD endpoint 105 may include a processing unit 205, a memory 210, an input device 215, an output device 220, a quantum cryptographic transceiver 225, a network interface(s) 230 and a bus 235. Processing unit 205 may perform all data processing functions for inputting, outputting, and processing of QKD endpoint data. Memory 210 may include Random Access Memory (RAM) that provides temporary working storage of data and instructions for use by processing unit 205 in

performing processing functions. Memory 210 may additionally include Read Only Memory (ROM) that provides permanent or semi-permanent storage of data and instructions for use by processing unit 205. Memory 210 can also include non-volatile memory, such as an electrically erasable programmable read only memory (EPROM) that stores data for use by processing unit 205. Memory 210 can further include a large-capacity storage device(s), such as a magnetic and/or optical recording medium and its corresponding drive.

[0031] Input device 215 permits entry of data into QKD endpoint 105 and may include a user interface (not shown). Output device 220 permits the output of data in video, audio, or hard copy format. Quantum cryptographic transceiver 225 may include mechanisms for transmitting and receiving cryptographic keys using quantum cryptographic techniques. Network interface(s) 230 may interconnect QKD endpoint 105 with network 110. Bus 235 interconnects the various components of QKD endpoint 105 to permit the components to communicate with one another.

Exemplary Quantum Cryptographic Transceiver

[0032] Fig. 3 illustrates exemplary components of quantum cryptographic transceiver 225 of a QKD endpoint 105 consistent with the present invention. Quantum cryptographic transceiver 225 may include a QKD transmitter 305 and a QKD receiver 310. QKD transmitter 305 may include a photon source 315 and a phase/polarization/ modulator 320. Photon source 315 can include, for example, a conventional laser. Photon source 315 may produce photons according to instructions provided by processing unit 205. Photon source 315 may produce photons of light with wavelengths

throughout the electromagnetic spectrum, including light in the human visible spectrum and light beyond the human-visible spectrum, such as, for example, infrared or ultraviolet light. Phase/polarization/ modulator 320 can include, for example, conventional Mach-Zehnder interferometers. Phase/polarization/ modulator 320 may encode outgoing photons from the photon source according to commands received from processing unit 205 for transmission across an optical link, such as link 115.

[0033] QKD receiver 310 may include a photon detector 325 and a photon evaluator 330. Photon detector 325 can include, for example, conventional avalanche photo detectors (APDs) or conventional photo-multiplier tubes (PMTs). Photon detector 325 can also include cryogenically cooled detectors that sense energy via changes in detector temperature or electrical resistivity as photons strike the detector apparatus. Photon detector 325 can detect photons received across the optical link. Photon evaluator 330 can include conventional circuitry for processing and evaluating output signals from photon detector 325 in accordance with quantum cryptographic techniques.

[0034] It will be appreciated that many other forms of quantum cryptographic transceivers may be employed in place quantum cryptographic transceiver 225. For instance, a transceiver may include only photon source 315, or only photon detector 325 and photon evaluator 330. As another example, so-called "plug and play" systems may be employed in which one transceiver includes photon source 315, photon detector 325, and photon evaluator 330, and another transceiver includes phase/polarization modulator 320 and a Faraday mirror (not shown). Alternatively, a transceiver may be based on so-called "entanglement-based" quantum cryptography, in which sets of entangled photons are used instead of single photons.

Exemplary QKD Endpoint Functional Block Diagram

[0034] Fig. 4 illustrates an exemplary functional block diagram 400 of a QKD endpoint 105 consistent with the present invention. Functional block diagram 400 may include QKD protocols 405, client(s) 410, optical process control 415, shared bits reservoir 420, a security policy database (SPD) 425, and a security association database (SAD) 430. QKD protocols 405 (collectively called secret bits producer) may further include an interface layer 440, a sifting layer 445, an error correction layer 450, a privacy amplification layer 455 and an authentication layer 460. The interface layer 440 may include protocols for deriving QKD symbols from photons transmitted via QKD link/network 115 and received at a quantum cryptographic transceiver 225 of a QKD endpoint 105. Values of the QKD symbols (e.g., high or low symbol values) may be interpreted at layer 440 by the polarization, phase or energy states of incoming photons. Interface layer 440 may measure the polarization, phase or energy state of each received photon and interpret the measurement as corresponding to whether a first detector fired, a second detector fired, both first and second detectors fired, neither detectors fired, or any other relevant measurements such as the number of photons detected.

[0035] Sifting layer 445 may implement protocols for discarding or "sifting" certain of the raw symbols produced by layer 440. The protocols of sifting layer 445 may exchange basis information between the parties to a QKD symbol exchange. As an example, when QKD endpoint 105a receives polarized photons from QKD endpoint 105b, sifting layer 445 may measure the polarization of each photon along either a rectilinear or diagonal basis with equal probability. Sifting layer 445 may record the basis that is used for measuring the polarization of each photon. Sifting layer 445 may

inform QKD endpoint 105b of the basis chosen for measuring the polarization of each photon. QKD endpoint 105b may then, via the protocols of sifting layer 445, inform QKD endpoint 105a, whether it has made the polarization measurement along the correct basis. QKD endpoint 105a and 105b may then "sift" or discard all polarization measurements in which QKD endpoint 105a has made the measurement along the wrong basis and keep only the measurements in which QKD endpoint 105a has made the measurement along the correct basis. For example, if QKD endpoint 105b transmits a photon with a symbol encoded as a 0° polarization and if QKD endpoint 105a measures the received photon via a diagonal basis (45° - 135°), then QKD endpoint 105b and 105a will discard this symbol value since QKD endpoint 105a has made the measurement along the incorrect basis.

[0036] Error correction layer 450 may implement protocols for correcting errors that may be induced in transmitted photons due to, for example, the intrinsic noise of the quantum channel. Layer 450 may implement parity or cascade checking, convolutional encoding or other known error correction processes. Error correction layer 450 may additionally implement protocols for determining whether eavesdropping has occurred on the quantum channel. Errors in the states (e.g., polarization, phase or energy) of received photons may occur if an eavesdropper is eavesdropping on the quantum channel. To determine whether eavesdropping has occurred during transmission of a sequence of photons, QKD endpoint 105a and QKD endpoint 105b may randomly choose a subset of photons from the sequence of photons that have been transmitted and measured on the same basis. For each of the photons of the chosen subset, QKD endpoint 105b publicly announces its measurement result to QKD endpoint 105a. QKD endpoint 105a then

informs QKD endpoint 105b whether its result is the same as what was originally sent. QKD endpoint 105a and 105b both may then compute the error rate of the subset of photons. If the computed error rate is higher than an agreed upon tolerable error rate (typically about 15%), then QKD endpoint 105a and 105b may infer that substantial eavesdropping has occurred. They may then discard the current polarization data and start over with a new sequence of photons.

[0037] Privacy amplification layer 455 may implement protocols for reducing error-corrected symbols received from layer 450 to a small set of derived symbols (e.g., bits) to reduce an eavesdropper's knowledge of the key. (In some technical literature, this specific step is known as "advantage distillation," although the term "advantage distillation" is more widely used in the broader sense defined in this application.) If, subsequent to sifting and error correction, QKD endpoint 105a and 105b have adopted n symbols as secret symbols, then privacy amplification layer 455 may compress the n symbols using, for example, a hash function. QKD endpoint 105a and 105b may agree upon a publicly chosen hash function f and take $K = f(n \text{ symbols})$ as the shared r-symbol length key K. The hash function randomly redistributes the n symbols such that a small change in symbols produces a large change in the hash value. Thus, even if an eavesdropper determines a number of symbols of the transmitted key through eavesdropping, and also knows the hash function f, they still will be left with very little knowledge regarding the content of the hashed r-symbol key K.

[0038] Authentication layer 460 may implement protocols for authenticating transmissions between QKD endpoint 105a and 105b via network 110. Such protocols

may include any conventional authentication mechanisms known to one skilled in the art (e.g., message authentication codes (MACs)).

[0039] Client(s) 410 may include one or more clients that perform various QKD endpoint functions. In one implementation, client(s) 410 may include one or more Internet Key Exchange (IKE) clients that implement key exchange protocols and algorithms. In another implementation, client(s) 410 may include one or more pseudo-random number generators that use deterministic functions that accept secret random numbers as seed values to produce pseudo-random number sequences. Client(s) 410 may retrieve, via client interface 465, secret bit symbols from shared bits reservoir 420 and provide the retrieved symbols, via peer interface 470, to a client associated with another QKD endpoint. Client interface 465 may be internal to a QKD endpoint 105 (e.g., shared via shared memory or local network link). Peer interface 470 may include an external communications channel through network 110.

[0040] Optical process control 415 may control opto-electronics of quantum cryptographic transceiver 225. In exemplary embodiments that use framing, optical process control 415 may impose the framing on the QKD link. Optical process control 415 may continuously transmit and receive frames of QKD symbols and report the results to QKD protocol suite 405. Shared bits reservoir 420 may reside in memory 210 and may store the secret cryptographic key symbols (i.e., "bits") derived via QKD protocols 405 (secret bits producer). Shared bits reservoir 420 may, in some implementations, comprise multiple shared bits reservoirs, one for each quantum cryptographic peer.

[0041] SPD 425 may include a database, together with algorithms, that classify received data units to determine which data belong in which security associations. This

may be accomplished by matching various fields in the received data units with rule sets in the database. SAD 430 may include a database, together with algorithms, that perform Internet Protocol Security (IPsec) algorithms on data units as needed for a given security association (e.g., encryption, decryption, authentication, encapsulation).

Exemplary High-Level System Diagram

[0042] Fig. 5 is an exemplary high-level system diagram, consistent with the present invention, that illustrates client selection and retrieval of secret bit values from shared bits reservoir 420 at each QKD endpoint 105a and 105b that is party to an cryptographic key exchange via QKD. Each QKD endpoint 105 may include one or more clients 410-1 through 410-N coupled to a shared bits reservoir 420 via a client interface 465. Any of clients 410-1 through 410-N may reserve a flow of secret bit values from the shared bits reservoir 420. Shared bits reservoir 420 may include multiple blocks of the secret bit values stored in one or more memory devices, such as memory 210 (Fig. 2). Each block may contain a series of secret bit values. The block of the multiple blocks may be organized into fixed-size or variable-size blocks. Blocks *i* 505, *j* 510, *k* 515 and *n* 520 are shown by way of example, though more or fewer numbers of blocks may be present in shared bits reservoir 420. An identification of a selected block of secret bits at one QKD endpoint 105a may be sent, via peer interface 470, to another QKD endpoint 105b. The selected block of secret bits may, for example, then be used for cryptographically protecting traffic sent via network 110 between QKD endpoint 105a and QKD endpoint 105b.

Reservations

[0043] Fig. 6 illustrates an exemplary reservation table 400, associated with a peer, such as one of clients 410-1 through 410-N, that may be maintained in each QKD endpoint 105 by a secret bits producer, such as QKD Protocols 405. A number of such reservation tables 600 may be maintained in each QKD endpoint 105, where each reservation table 600 is associated with a different client peer 410 (Fig. 4). Exemplary reservation table 600 may include a peer ID 602, an estimated production rate 604, an available rate 606, a number of reservations 608, and reservation information 610-1 through 610-n for a number of reservations (n) indicated by # reservations 608. Each item of reservation information 610-1 through 610-n may include a reservation ID 610-a, a priority 610-b and a rate 610-c, which may be in bits per second or any other convenient unit of measurement.

[0044] Peer ID 602 may refer to associated client peer 410, for example, from a perspective of QKD endpoint 105a, client B1, B2 or BN of QKD 105b (Fig. 5). Estimated production rate 604 may store a value representing an estimate of how fast secret bits are being accumulated with client peer 410. Available rate 606 may store a value representing the estimated production rate minus the sum of the rates for all current reservations in this table associated with a particular peer ID 602. The # reservations field 608 may store a value indicating the number of reservations that are currently active in the table for a particular client peer. In this example, # reservations 408 indicates that n reservations are currently active for a client peer indicated by peer ID 602.

Exemplary REQUEST Message

[0045] A REQUEST message may be sent from a client to a secret bits producer, for example, QKD protocols 405, when a reservation is desired. Fig. 7 illustrates an exemplary format of a REQUEST message 700 in an implementation consistent with the present invention. REQUEST message 700 may include a type field 702, a peer ID field 704, a priority field 706, a minimum acceptable rate field 708, and a desired rate field 710.

[0046] Type field 702 identifies a message type. For example, type field 702 may identify the message as a REQUEST message. Peer ID field 704 may store an identifier for a peer. In one implementation, the identifier may be a network address. Priority field 706 may store an indication of a priority of the reservation. In one implementation, for example, a low priority may be 1, a medium priority may be 2, and a high priority may be 3. Other priority schemes may be used in other implementations. Minimum acceptable rate field 708 may indicate a lowest acceptable rate for a reservation such as, for example, 100 bits per second. Desired rate field 710 may indicate a desired requested rate such as, for example, 500 bits per second.

Exemplary REPLY Message

[0047] Fig. 8 illustrates an exemplary format of a REPLY message 800 that may be sent by the secret bits producer to the client to indicate a success, partial success, or failure of a reservation request. REPLY message 800 may include a type field 702, a reservation ID field 804 and an achieved rate field 806.

[0048] Type field 702 may indicate a message type. In this situation, REPLY message 800 may store an identifier that indicates that the message 800 is a REPLY

message. Reservation ID field 804 may include a reservation identifier created by a secret bits producer, such as QKD protocols 405, for this particular reservation. Achieved rate field 806 may be zero or a number from a minimum acceptable rate to a desired rate. A value of zero may be a failure indication and a value greater than or equal to the minimum acceptable rate, but less than the desired rate may indicate a partial-success. A value equal to the desired rate may indicate a full-success.

[0049] A secret bits producer, for example, QKD protocols 405, may inspect a received REQUEST message and determine if the requested rate is available by inspecting reservation table 600 for the appropriate peer. If the reservation can be fully or partially satisfied, the secret bits producer may add new reservation information 610 to reservation table 600 and may return an appropriate indication, either full-success or partial-success to the requesting client. Otherwise, the secret bits producer may return a failure indication in REPLY message 800 to the requesting client.

Exemplary DONE Message

[0050] A client may send a DONE message to a secret bits producer, such as QKD protocols 405, when the reservation is no longer needed. The secret bits producer may then remove the reservation from the appropriate reservation table.

[0051] Fig. 9 illustrates an exemplary format of a DONE message 900. DONE message 900 may include a type field 702, a peer ID field 704 and reservation ID field 804.

[0052] Type field 702 may indicate a message type. In this situation, the DONE message 900 may store an identifier that indicates that the message 900 is a DONE message. Peer ID field 704 may identify a peer, for example, client B1 (Fig. 5).

Reservation ID field 804 may include a reservation identifier created by a secret bits producer, such as QKD protocols 405, for this particular reservation.

[0053] Other messages may also be used in various implementations. For example, an error message may be issued by a secret bits producer, such as QKD protocols 405, if a DONE message contains an invalid reservation ID. An invalid reservation ID is a reservation ID that cannot be found in reservation table 600 for a particular peer. A variant of the REPLY message may be used as a format for the error message. Instead of having an achieved rate field, the error message may have an error code field. Further, a CHANGE-RESERVATION message may be used in some implementations. Such a message may be sent by a client to a secret bits producer, such as QKD protocols 405, to alter priority and/or a rate for a given reservation. The format of the CHANGE-RESERVATION message may be a variant of the REQUEST message.

Estimated Production Rate

[0054] A conservative estimated production rate of a number of bits per second that may be produced by a secret bits producer may be used with implementations consistent with the principles of the invention. Such a conservative estimated production rate may tend to underestimate the actual production rate. Thus, on average, all bits that are actually produced during most periods of operation are not reserved. At least some of the left-over bits may be used on demand in a first-come, first-served manner. If the left-over bits are not used, they may be stockpiled for use during "lean periods" of bit production.

[0055] In one implementation consistent with the principles of the invention, estimated production rate may be a 10^{th} percentile of observed production rates over a

previous K observation intervals, for example, K may be 120 and each observation interval may be 1 minute. In this implementation, the secret bits producer, for example, QKD protocols 405, may measure the actual bit production rate over each production interval (1 minute). The secret bits producer may keep a record of the most recent K (120) observations. If the secret bits producer uses the 10^{th} percentile of observed production rate as the estimated production rate, the 12^{th} from the lowest measured production rate over the past two hours is selected as the estimated production rate (assuming 120 observations (1 minute each)). Because the observed rate may be in units of bits per minute, the selected value may then be normalized to bits per second by dividing by 60. The resulting value may then be used as estimated production rate 604.

[0056] In other implementations, the secret bits producer may use another percentile of observed production rates, K may be a value other than 120, and the observation interval may be an interval other than 1 minute. It should also be noted that many different estimation algorithms may be used in various implementations consistent with the principles of the invention.

Exemplary Estimated Production Rate Update Process

[0057] Fig. 10 is a flowchart that illustrates an exemplary process performed by a secret bits producer, such as QKD protocols 405, to update an estimated production rate. The secret bits producer may wait during an observation time interval for a given peer (act 1002). QKD protocols 405 may maintain an observation table including a number of entries X, for example, X may be 120. Each entry may include a number of bits produced during a respective observation interval. After waiting during the observation interval, an oldest observation table entry may be replaced with a number of bits

produced during a most recent observation interval (act 1004). The secret bits producer may then compute a K^{th} percentile of values stored in the observation table (act 1006). The secret bits producer may store the computed value in estimated production rate 604 for the peer (act 1008). The secret bits producer may adjust available rate 606 upward or downward, accordingly, based on the estimated production rate 604 (act 1010). The secret bits producer may then determine whether the available rate is less than zero (act 1012). If the available rate is not less than zero, then the procedure is completed. Otherwise, the secret bits producer may find the lowest priority reservation for the given peer by examining priority 610-1b through 610-nb in the reservation table 600 associated with a particular peer (act 1014) and deleting the associated reservation information 610 (act 1016). The secret bits producer may again adjust the available rate (act 1010). The secret bits producer may repeat acts 1014, 1016 and 1010 until the available rate is not less than zero (act 1012). Thus, the secret bits producer may delete lowest priority reservations when the available rate is negative until the available rate becomes non-negative.

Exemplary Reservation Handling Process

[0058] Figs. 11, 12A and 12B are flowcharts that illustrate exemplary processing in a secret bits producer, such as QKD protocols 405, when a REQUEST message is received. First, the secret bits producer may determine whether peer ID in peer ID field 704 is valid (act 1102). The secret bits producer may determine the validity of a peer ID by examining peer ID field 602 in each reservation table 600 associated with a peer. If a matching peer ID cannot be found, then the value in peer ID field 704 is not valid. If the

value in peer ID field 704 is not valid, the secret bits producer may discard the REQUEST message and return an error reply to the client (act 1104).

[0059] If the peer ID in peer ID field 704 is valid, the secret bits producer may then check whether a value in priority field 706 of the REQUEST message is valid (act 1106). There may be a range of priority values that may be valid, for example, 1-3. If a priority value is outside the valid range, it is not valid. If the value in priority field 706 is not valid, the secret bits producer may discard the REQUEST message and send an error reply to the client (act 1108).

[0060] If the value in priority field 706 is valid, the secret bits producer may then check whether a value in minimum acceptable rate field 708 and desired rate field 710 of the REQUEST message are valid (act 1110). Minimum acceptable rate field 708 and desired rate field 710 may each have a valid range of values, for example, 10-100 and 300-1200, respectively. If either a value in minimum acceptable rate field 708 or a value in desired rate field 710 is not valid, then the secret bits producer may discard the REQUEST message and send an error reply to the client (act 1112).

[0061] If the value in minimum acceptable rate field 708 and desired rate field 710 are valid, then the secret bits producer may determine whether the value in minimum acceptable rate field 708 is less than or equal to the value in desired rate field 710 (act 1114). If the value in minimum acceptable rate field 708 is not less than or equal to the value in desired rate field 710, then the secret bits producer may discard the REQUEST message and send an error reply to the client (act 1116).

[0062] If the value in minimum acceptable rate field 708 is less than or equal to the value in desired rate field 710 (act 1114), the secret bits producer may then determine

whether available rate 606 (Fig. 6) for the appropriate peer is less than the value in minimum acceptable rate field 708 (act 1118). If the value of available rate 606 for the appropriate peer is not less than the value in minimum acceptable rate 708 then the secret bits producer may set a value of achieved rate field 806 of a REPLY message to the lesser of a value in desired rate field 710 and a value in available rate field 606 for the appropriate peer (act 1120).

[0063] The secret bits producer may then adjust the value in available rate 606 for the appropriate peer by subtracting the value in achieved rate field 806 from the value in available rate 606 (act 1202; Fig. 12A). The secret bits producer may then create a new reservation information entry 610 for the reservation and may return a value in reservation ID field 804 in the REPLY message to the client (acts 1204 and 1206).

[0064] If the secret bits producer determines that the value in available rate 606 for the appropriate peer is less than the value in minimum acceptable rate field 708 (act 1118), the secret bits producer may compute S, the sum of achieved rates for lower priority reservations for the appropriate peer (act 1208; Fig. 12B). The secret bits producer may compute S by examining priority fields 610-1c through 610-nc in reservation table 600 for the appropriate peer. If a value in a respective priority field 610-b is less than the value in priority field 706, the secret bits producer may add a corresponding rate 610-c to S. The secret bits producer may then determine whether S is greater than or equal to the value in minimum acceptable rate field 708. If S is not greater than or equal to the value in minimum acceptable rate 708, the secret bits producer may send a REPLY message to the client with a value of zero in achieved rate field 806, indicating failure (act 1212). Otherwise, the secret bits producer may delete a

reservation having lowest priority (act 1214) by finding a priority field 610-b with a lowest priority value in reservation table 600 for the appropriate peer and changing the value of fields 610 to indicate that the fields are deleted. The secret bits producer may then add the old value of rate field 610-c, corresponding to the lowest priority reservation for the peer, to available rate field 606 . The secret bits producer may then either repeat acts 1118-1214 if the value in available rate field 606 is less the value in minimum acceptable rate field 708, or the secret bits producer may perform acts 1120, and 1202-1206 if the value in available rate field 606 is not less than the value in minimum acceptable rate field 708.

Exemplary Reservation Deletion Process

[0065] Fig. 13 illustrates a flowchart of a procedure that may be performed by a secret bits producer, such as QKD protocols 405, when a DONE message is received from a client. The exemplary process begins with the secret bits producer determining whether a value in peer ID field 704 (Fig. 9) is valid (act 1302). The value in peer ID field 704 is valid if the value can be found in Peer ID field 602 of one of the reservation tables 600. Otherwise, the value in peer ID field 704 is not valid. If the value in peer ID field 704 is not valid, the procedure may end. Alternatively, the secret bits producer may return an error reply to the client.

[0066] If the value in peer ID field 704 is valid, the secret bits producer may determine whether a value in reservation ID field 804 (Fig. 9) is valid (act 1303). The value in reservation ID field 804 is valid if the value can be found in field 610-a of an active reservation information entry for an appropriate peer. Otherwise the value in reservation ID field 804 is not valid. If the value in reservation ID field 804 is not valid,

the procedure may end. Alternatively, the secret bits producer may return an error reply to the client.

[0067] If the value in reservation ID field 804 is valid, then the secret bits producer may delete the appropriate reservation from reservation table 600 for the peer (act 1304) by changing the active entry 610 having a matching reservation ID 610-1 to indicate a deleted entry. The secret bits producer and may adjust available rate 604 by adding a value in rate field 610-c of the deleted reservation entry to available rate 604 (act 1306).

Hard State vs. Soft State

[0068] Networking experts may consider the above-described approach a so-called "hard state" approach to reservations because once a client has made a reservation, the secret bits producer, for example, QKD protocols 405, may correctly maintain the reservation for an unbounded period of time.

[0069] Networking experts may consider the following alternative reservation approach to be a so-called "soft state" approach because a reservation lasts for a limited period of time unless it is periodically renewed by the client. Thus, when a client desires to maintain a particular reservation, the client would repeat sending a REQUEST message from time to time. If the reservation is not renewed, it is deleted from the reservation table 400 after the limited amount of time.

Modifications and Variations

[0070] In some implementations, a secret bits producer, for example, QKD protocols 405, may determine whether a client is using more bits than it has reserved. If this is the case, the secret bits producer may take some action. For example, the secret bits producer may not provide secret bits to the client beyond the reserved rate or the secret

bits producer may provide the bits, but may also send an error reply including a warning to the client informing the client that it is exceeding the reserved rate.

[0071] In other implementations, a secret bits producer, for example, QKD protocols 405, may monitor a rate at which bits are consumed. If the bits are being consumed by an "unreserved" client, the bits will be provided to the "unreserved" client if they are available. The bits will not be provided to the "unreserved" clients if they are needed to satisfy a reservation. Thus, bits may be reserved for some services, and other services may receive bits on a best effort basis from bits that remain after all reservations have been satisfied.

[0072] Embodiments of the invention may be implemented in hardware, software, or firmware. The firmware may be in a Read-Only Memory (ROM) and the software may reside on, for example, a medium such as a floppy disk, optical disk, or CD ROM.

Other Considerations

[0073] The above-described methods and systems may be applied to any system that is based on advantage distillation. Further, although implementations have been described using a secret bits producer, such as QKD protocols 405, implementations consistent with the principles of the invention may be used with any system based on an application that produces bits for other applications or clients that consume bits.

[0074] Further, clients 410-1 through 410-N may include software entities that communicate with QKD protocols 405 via an Inter-Process Communication (IPC) technique. The IPC may be the well-known Common Object Request Broker Architecture (CORBA), although many other IPC techniques may be used instead such as, for example, remote procedure calls, well-known Internet protocols, such as

Transmission Control Protocol/Internet Protocol (TCP/IP) and User Datagram Protocol/Internet Protocol (UDP/IP), and communications through shared memory.

Conclusion

[0075] Methods and systems consistent with the principles of the invention allow a secret bits consuming application to reserve bits from a secret bits producing application. The methods and systems may be used with any applications that produce bits and with any applications that consume bits.

[0076] The foregoing description of preferred embodiments of the invention provides illustration and description, but is not intended to be exhaustive or to limit the invention to the precise form disclosed. Modifications and variations are possible in light of the above teachings or may be acquired from practice of the invention for example, while a series of acts has been described with regard to Figs. 10-13, the order of the acts may differ in other implementations consistent with the present invention. Also, non-dependent acts may be performed in parallel.

[0077] No element, act, or instruction used in the description of the present application should be construed as critical or essential to the invention unless explicitly described as such. Also, as used herein, the article "a" is intended to include one or more items. Where only one item is intended, the term "one" or similar language is used. The scope of the invention is defined by the claims and their equivalents.